IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Cheh Goh, Liqun Chen, Stephen J. Crane, Marco C. Mont, and Keith A. Harrison		
Assignee:	Hewlett-Packard Development Company, L.P.		
Title:	Data Output Method, System and Apparatus		
Serial No.:	10/664,069	Conf. No.	3247
Examiner:	Beemnet W. Dada	Group Art Unit:	2435
Docket No.:	300110535-2	Filing Date:	September 16, 2003

November 16, 2009

Mail Stop APPEAL
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. §§ 1.191 AND 41.67

Dear Sir:

Appellants submit this Appeal Brief pursuant to the Notice of Appeal filed in the above-identified patent application on September 16, 2009.

I. REAL PARTY IN INTEREST

The real party in interest is the assignee, Hewlett-Packard Development Company, L.P., as named in the caption above.

II. RELATED APPEALS AND INTERFERENCES

Based on information and belief, there are no prior or pending appeals, interferences or judicial proceedings known to Appellant, the Appellant's legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

III. STATUS OF CLAIMS

Claims 1-38 are pending in this case and are reproduced below in an Appendix below. Claims 39 and 40 were previously canceled. Claims 1-4, 11-18, 25-28, 30, 31, and 35-38 and

stand rejected and are the subject of this appeal. Claims 5-10, 19-24, 29, and 32-34 stand objected to.

IV. STATUS OF AMENDMENTS

There are no unentered amendments in this case. No amendments were filed subsequent to the final rejection dated June 16, 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates to protection of information that might be output to a removable medium. For example, some embodiments of the invention implement security policies for printing of information. Embodiments of the invention can employ Identifier Based Encryption (IBE) using a representation of a security policy as the identifier string in the IBE that encrypts the information to be protected from unauthorized output. An output device then needs a decryption key before the information can be decrypted and output in unencrypted or plain text form. These embodiments can reduce or avoid the chance of a security breach that might result from a malicious attempt to provide altered security policy information to a trusted authority that can provide a key for decrypting the information. In particular, the trusted authority must be provided with the correct policy information in order to generate the correct decryption key. Accordingly, the trusted authority can check compliance with the correct security policy before providing a decryption key.

Independent claim 1 is directed to a system such as illustrated in Fig. 3 including: "an output device for outputting data onto a removable storage medium," e.g., printer 30; "a first computing entity for encrypting a first data set," e.g., the user's computing entity 20; and "a second computing entity associated with the trusted party," e.g., computing entity 21.

The first computing entity 30 encrypts the first data set, e.g., encrypts a document to be printed as described in paragraph [0049]. The parameters used in the encryption includes: "public data of a trusted party," e.g., a public key *R*, and "an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium," e.g., string *ID*. Paragraph [0049] describes how computing entity 20 can encrypt a document for printing using a representation of the policy as an encryption key string in an IBE (Identifier-Based Encryption) process. Paragraphs [0056] to [0081] describe an IBE process in detail. Paragraph [0067] particularly describes encryption using an identifier based public key Q_{ID}/private key S_{ID} pair, where $S_{ID}=sQ_{ID}$, s is a secret of

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

the trusted authority, and Q_{ID} is the public key for identifier string ID that represents the policy for printing the encrypted document. The first computing entity is "further arranged to output the encrypted first data set for the output device," e.g., entity 20 forwards the cipher text to printer 30 as described in paragraph [0050].

The second computing entity 21 is "arranged when satisfied that said policy has been met, to output for the output device a decryption key, distinct from the encryption key string, for use in decrypting the encrypted first data set," as described in paragraph [0055]. The second computing entity is "arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data." A decryption key S_{print} as described in paragraph [0084] depends on the public key $Q_{print}=Q_{ID}$ and therefore depends on the encryption key string ID. Claim 1 finishes by reciting, "the output device being arranged to use the decryption key in decrypting the encrypted first data set" as described in paragraph [0053].

Independent claim 15 is directed to a data output method that includes, "(a) encrypting a first data set," e.g., encrypting a document for printing as described in paragraph [0049]. The encrypting is "based on encryption parameters that comprise: i. public data of a trusted party, and ii. an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set to a removable storage medium." The public and private data of an identifier based encryption process is described in paragraphs [0056] to [0081], and use the policy, or a representation of the policy, as an encryption key string in an IBE as described in paragraph [0049]. Step (b), "providing the encrypted first data set to an output device adapted to output data to a removable storage medium," corresponds in the embodiment illustrated in Fig. 3 to a user's computing entity 20 providing encrypted data to a printer 30 as described in paragraph [0050]. Step (c), "at the trusted party checking that said policy has been satisfied and thereafter providing the output device with a decryption key, distinct from the encryption key string, for use in decrypting the encrypted first data set, this decryption key being generated in dependence on the encryption key string and private data related to said public data" corresponds in the embodiment of Fig. 3 to trust authority computing entity 21 checking for compliance with the policy as described in paragraph [0055] and generating a decryption key, for example, as described in paragraph [0084]. Final step (d), "at the output device using the decryption key in decrypting the encrypted first data set and outputting the first data set to a removable recording medium" is described in paragraph [0055] in regard to the decrypting and printing of a document.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

Independent claim 28 is specifically directed to a printing system. For example, the printing system illustrated in Fig. 3 includes: "a printer" e.g., printer 30; "a first computing entity for encrypting a first data set," e.g., computing entity 20; and "a second computing entity associated with the trusted party," e.g., computing entity 21. The first computing entity encrypts the first data set based on encryption parameters that comprise: i. public data of a trusted party, and ii. an encryption key string comprising a second data set that defines a policy for allowing the printing of the first data set. See paragraphs [0056] to [0081]. The first computing entity is further arranged to output the encrypted first data set for the printer as described in paragraph [0050], The second computing entity is "arranged when satisfied that said policy has been met, to output for the printer a decryption key, distinct from the encryption key string, for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data." See paragraphs [0055] and [0084] as noted above. Finally, "the printer being arranged to use the decryption key in decrypting the encrypted first data set" is described in paragraph [0055].

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following issue is presented to the Board of Patent Appeals and Interferences for decision:

> Whether Claims 1-4, 11-18, 25-28, 30, 31, and 35-38 are unpatentable under 35 U.S.C. 103(a) over U.S. Pat. App. Pub. No. 2002/0013772 A1 (hereinafter Peinado) in view of U.S. Pat. App. Pub. No. 2003/0196099 A1 (hereinafter Lampson).

VII. ARGUMENT

> Claims 1-4, 11-18, 25-28, 30, 31, and 35-38 are patentable under 35 U.S.C. 103(a) over Peinado in view of Lampson.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

Independent claim 1 distinguishes over the combination of Peinado and Lampson at least by reciting, "a first computing entity for encrypting a first data set, the first computing entity encrypting the first data set based on encryption parameters that comprise: public data of a trusted party, and an encryption key string comprising a second data set that defines a

policy for allowing the output of the first data set onto a said removable storage medium." The combination of Peinado and Lampson fails to suggest encryption based on an encryption key string that defines a policy for allowing output.

Peinado discloses processes that restrict rendering of content to users that have obtained licenses. In an exemplary process disclosed by Peinado, the content is encrypted and can be decrypted using a decryption or content key KD. A user obtains a license 16 or a sub-license 16s that includes the content key in an encrypted form that the user/device can decrypt. The licensed user can use a private key to decrypt the content key KD included in the license or sub-license and can then use the content key KD to decrypt and render the licensed content. See, for example, Peinado paragraph [0044]. Peinado also discloses a user obtaining a sub-license 16s, e.g., for a portable device, based on a previously obtained license 16 for a home device. However, while content key KD may be included with a license 16 or sub-license 16s, neither the license nor the sub-license suggests an encryption key string as recited in claim 1.

The Final Office Action cited paragraph [0278] and paragraphs [0284] to [0292] of Peinado when responding to Appellants' prior remarks regarding the failure of Peinado to teach or suggest encryption "based on encryption parameters that comprise: … an encryption key string … that defines a policy for allowing the output." The Final Office Action particularly notes that "the content key is re-encrypted and tied to the license (policy)" as described in paragraph [0278] of Peinado. Appellants assert that decrypting a content key contained in a license and then re-encrypting the content key for inclusion in a sub-license or policy in no way suggests that the license (or a policy) is an encryption key string for either the encryption or the re-encryption. Paragraph [0278] describes that content key KD in the license 16 is encrypted using a first scheme, e.g., PU-BB-CO, and the content key KD in the sub-license is encrypted using a second scheme, e.g., PU-BB-PD. The two encryption schemes respectively correspond to the different devices that are able to decrypt the content key KD from the license and sub-license. As noted above, Peinado teaches tying the encrypted content key to a license or sub-license by including the encrypted content key in the license 16 or sub-license 16s, but Peinado fails to suggest using the license or sub-license as a parameter of either encryption process.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

In accordance with an aspect of Applicants' invention, Identity Based Encryption (IBE) can use an encryption key string that defines a policy for control of output, so that the encryption/decryption depends upon the policy with which output must comply. Accordingly,

a trusted authority cannot be tricked into providing the correct decryption key in response to checking the wrong policy. Further, with the invention of claim 1, decryption and output are inherently related to the output policy, and determining the appropriate policy does not require encryption of content and then a different encryption of a decryption key, as does the process of Peinado.

Lampson is cited for disclosing encryption/decryption processes that use distinct encryption and decryption keys. Otherwise, Lampson like Peinado discloses encrypting the conditions required for allowing decryption of desired content. (See, for example, the abstract of Lampson.) Accordingly, the combination of Peinado and Lampson does not suggest "encryption parameters that comprise: … an encryption key string … that defines a policy for allowing the output" as recited in claim 1.

In Graham v. John Deere Co. of Kansas City, 383 U. S. 1, 17-18 (and more recently in KSR International Co. v. Teleflex Inc., 550 USPQ2d 1385 (2007), the U.S. Supreme Court set forth analysis used in applying 35 U.S.C. §103. In accordance with Graham, "the scope and content of the prior art are ... determined; differences between the prior art and the claims at issue are ... ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined." In the present case, the combination of Peinado and Lampson discloses encrypting information using content key and providing decryption keys that are encrypted in a manner that a licensed user can decrypt. In contrast, claim 1 recites, "encryption parameters that comprise: … an encryption key string … that defines a policy for allowing the output." One of ordinary skill in the art in view of claim 1 and Appellants' disclosure would understand that "an encryption key string" as used in Identity Based Encryption controls the manner of encryption, and the combination Peinado and Lampson fails to lead one of ordinary skill in the art to leap to the idea of using an output policy as an encryption key string. Instead, the cited art teaches encrypting keys according to the recipient/licensee. Accordingly, claim 1 is patentable over the combination of Peinado and Lampson.

Claims 2-4 and 11-14 depend from claim 1 and are patentable over Peinado and Lampson for at least the same reasons that claim 1 is patentable over Peinado and Lampson.

Independent claim 15 distinguishes over the combination of Peinado and Lampson at least by reciting, "encrypting a first data set, said encrypting being based on encryption parameters that comprise: … an encryption key string ... that defines a policy for allowing the output of the first data set to a removable storage medium." For the reasons given above in

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

regard to claim 1, the combination of Peinado and Lampson does not suggest "encryption parameters that comprise: … an encryption key string … that defines a policy for allowing the output." Accordingly, claim 15 and claims 16-18 and 25-27, which depend from claim 15, are patentable over Peinado and Lampson.

Independent claim 28 similarly distinguishes over the combination of Peinado and Lampson at least by reciting, "encrypting the first data set based on encryption parameters that comprise: … an encryption key string comprising a second data set that defines a policy for allowing the printing of the first data set." For the reasons given in detail with reference to claim 1, Peinado and Lampson fail to suggest an encryption key string that defines a policy for allowing output or printing of data. Accordingly, claim 28 and claims 30, 31, and 35-38, which depend from claim 28, are patentable over Peinado and Lampson.

For the above reasons, Appellants submit the present rejection is unfounded and request that the rejections of claims 1-4, 11-18, 25-28, 30, 31, and 35-38 be reversed.

Claims 5-10, 19-24, 29, and 32-34 were objected to as being dependent on a rejected base but were indicated as being allowable if amended to independent form including the limitations of respective base claims and any intervening claims. For the same reasons that the rejection should be reversed as discussed above, the objection to claims 5-10, 19-24, 29, and 32-34 should be withdrawn.

Please contact the undersigned attorney at (530) 621-4545 if there are any questions concerning this Appeal Brief or the application generally.

Respectfully submitted,

/David Millers 37396/

David Millers
Reg. No. 37,396

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

VIII. CLAIMS APPENDIX

Claims 1-38 as currently pending are copied below.

1. (Previously Presented) A system comprising:

an output device for outputting data onto a removable storage medium;

a first computing entity for encrypting a first data set, the first computing entity encrypting the first data set based on encryption parameters that comprise:

public data of a trusted party, and

an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium,

the first computing entity being further arranged to output the encrypted first data set for the output device; and

a second computing entity associated with the trusted party and arranged when satisfied that said policy has been met, to output for the output device a decryption key, distinct from the encryption key string, for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data; the output device being arranged to use the decryption key in decrypting the encrypted first data set.

2. (Original) A system according to claim 1, wherein the second computing entity is arranged to generate the decryption key only when said policy has been met.

3. (Original) A system according to claim 1, wherein the second computing entity is arranged to issue to the first computing entity at least one of:

the second data set;

the encryption key string;

a derivative of the encryption key string usable by the first computing entity, in place of the encryption key string, in the encryption of said first data set.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

4. (Original) A system according to claim 1, wherein the second computing entity is arranged to receive the encryption key string directly or indirectly from the first computing entity.

5. (Original) A system according to claim 1, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising for the or each said further trusted party the public data of that trusted party and a respective further encryption key string that comprises further second data defining a further policy for allowing printing of the first data set; the or each further second computing entity being arranged, when satisfied that the policy defined by the encryption key string related to the associated trusted party has been met, to provide a further decryption key to the output device, the second computing entity concerned being arranged to generate this further decryption key in dependence on the private data and encryption key string corresponding to the associated trusted party; and decryption of the encrypted first data set by the output device requiring use of the decryption keys provided by all of the trusted parties.

6. (Original) A system according to claim 5, wherein the first data set concerns a document to be published, the first computing entity and one of the second computing entities are both associated with a document publisher, and the output device is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the output device.

7. (Original) A system according to claim 5, wherein the first computing entity is arranged to process the first data set, prior to encryption, to form a plurality of data strings, the first computing entity being further arranged to encrypt each data string based on the encryption parameters associated with a respective one of the trusted parties, and the output device being arranged to decrypt each string using the decryption key provided by the related trusted party and then to process the strings to recover the first data set.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

8. (Original) A system according to claim 1, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising the public data of the or each further trusted party; each second computing entity being arranged, when satisfied

that the policy defined by the encryption key string has been met so far as the associated trusted party is concerned, to provide a respective decryption key to the output device, the second computing entity concerned being arranged to generate this decryption key in dependence on the encryption key string and the private data of the associated trusted party; and decryption of the encrypted first data set by the output device requiring use of the decryption keys provided by all of the trusted parties.

9. (Original) A system according to claim 8, wherein said policy comprises a respective set of at least one condition associated with the or each trusted party, each second computing entity being arranged to be satisfied that said policy has been met when the set of at least one condition for the trusted party associated with the second computing entity concerned has been met.

10. (Original) A system according to claim 8, wherein the first data set concerns a document to be published, the first computing entity and one of the second computing entities are both associated with a document publisher, and the output device is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the output device.

11. (Original) A system according to claim 1, wherein the first data set is encrypted using a bilinear pairing technique.

12. (Original) A system according to claim 1, wherein the first data set is encrypted using a quadratic residue technique.

13. (Original) A system according to claim 1, wherein the output device and the second computing entity are incorporated into the same item of equipment.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

14. (Original) A system according to claim 1, further comprising a portable device comprising the second computing entity and a first communications interface, the output

device comprising a second communications interface arranged to cooperate with the first communications interface to enable communication between the second computing entity and the output device; the communications interfaces being such that the portable device must be present at the output device for the communication between the second computing entity to take place.

15. (Previously Presented) A data output method comprising the steps of:

(a) encrypting a first data set, said encrypting being based on encryption parameters that comprise:

i. public data of a trusted party, and

ii. an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set to a removable storage medium,

(b) providing the encrypted first data set to an output device adapted to output data to a removable storage medium;

(c) at the trusted party checking that said policy has been satisfied and thereafter providing the output device with a decryption key, distinct from the encryption key string, for use in decrypting the encrypted first data set, this decryption key being generated in dependence on the encryption key string and private data related to said public data; and

(d) at the output device using the decryption key in decrypting the encrypted first data set and outputting the first data set to a removable recording medium.

16. (Original) A method according to claim 15, wherein in step (c) the decryption key is generated only after said policy has been satisfied.

17. (Original) A method according to claim 15, further comprising an initial step of generating the second data set at the trusted party and providing to a party that is to carry out step (a) at least one of:

the second data set;

the encryption key string;

a derivative of the encryption key string usable in step (a), in place of the encryption key string, in the encryption of said first data set.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

18. (Original) A method according to claim 15, wherein the trusted party receives the encryption key string directly or indirectly from a party that carries out step (a).

19. (Original) A method according to claim 15, wherein:

in step (a) said encryption parameters further comprise public data of at least one further trusted party and a respective related further encryption key string that comprises further second data defining a further policy for allowing printing of the first data set;

in step (c) the or each further trusted party, when satisfied that the policy defined by the related encryption key string has been met, provides a further decryption key to the output device, the further trusted party concerned generating this further decryption key in dependence on private data and said related encryption key string; and

in step (d) decryption of the encrypted first data set by the output device requires use of the decryption keys provided by all of the trusted parties.

20. (Original) A method according to claim 19, wherein:

the first data set concerns a document to be published;

step (a) is carried out by a document publisher who also serves as one of the trusted parties;

the output device is associated with a document seller;

in step (c) the trusted party associated with the document publisher checks satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and

in step (c) another of said trusted parties checks satisfaction of at least one condition concerning the output device.

21. (Original) A method according to claim 19, wherein:

in step (a) the first data set is processed, prior to encryption, to form a plurality of data strings, each string being thereafter encrypted based on the encryption parameters associated with a respective one of the trusted parties, and

in step (d) the output device decrypts each string using the decryption key provided by the related trusted party and then processes the strings to recover the first data set.

22. (Original) A method according to claim 15, wherein:

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

in step (a) said encryption parameters further comprise public data of at least one further trusted party;

in step (c) each trusted party, when satisfied that the policy defined by the encryption key string has been met so far as it is concerned, provides a respective decryption key to the output device, the further trusted party concerned generating this decryption key in dependence on private data and the encryption key string; and

in step (d) decryption of the encrypted first data set by the output device requires use of the decryption keys provided by all of the trusted parties.

23. (Original) A method according to claim 22, wherein said policy comprises a respective set of at least one condition associated with the or each trusted party, each trusted party being arranged to be satisfied that said policy has been met when the set of at least one condition associated with the trusted party has been met.

24. (Original) A method according to claim 22, wherein:

the first data set concerns a document to be published;

step (a) is carried out by a document publisher who also serves as one of the trusted parties;

the output device is associated with a document seller;

in step (c) the trusted party associated with the document publisher checks satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and

in step (c) another of said trusted parties checks satisfaction of at least one condition concerning the output device.

25. (Original) A method according to claim 15, wherein in step (a) the first data set is encrypted using a bilinear pairing technique.

26. (Original) A method according to claim 15, wherein in step (a) the first data set is encrypted using a quadratic residue technique.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

27. (Original) A method according to claim 15 wherein the trusted authority is implemented in a portable device arranged to communicate with the output device only when the portable device is present at the output device.

28. (Previously Presented) A printing system comprising:

a printer;

a first computing entity for encrypting a first data set, the first computing entity encrypting the first data set based on encryption parameters that comprise:

i. public data of a trusted party, and

ii. an encryption key string comprising a second data set that defines a policy for allowing the printing of the first data set,

the first computing entity being further arranged to output the encrypted first data set for the printer; and

a second computing entity associated with the trusted party and arranged when satisfied that said policy has been met, to output for the printer a decryption key, distinct from the encryption key string, for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data;

the printer being arranged to use the decryption key in decrypting the encrypted first data set.

29. (Original) A system according to claim 28, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising for the or each said further trusted party the public data of that trusted party and a respective further encryption key string that comprises further second data defining a further policy for allowing printing of the first data set; the or each further second computing entity being arranged, when satisfied that the policy defined by the encryption key string related to the associated trusted party has been met, to provide a further decryption key to the printer, the second computing entity concerned being arranged to generate this further decryption key in dependence on the private data and encryption key string corresponding to the associated trusted party; and decryption of the encrypted first data set by the printer requiring use of the decryption keys provided by all of the trusted parties.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

30. (Original) A system according to claim 29, wherein the first data set concerns a document to be published, the first computing entity and one of the second computing entities are both associated with a document publisher, and the printer is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the printer.

31. (Original) A system according to claim 29, wherein the first computing entity is arranged to process the first data set, prior to encryption, to form a plurality of data strings, the first computing entity being further arranged to encrypt each data string based on the encryption parameters associated with a respective one of the trusted parties, and the printer being arranged to decrypt each string using the decryption key provided by the related trusted party and then to process the strings to recover the first data set.

32. (Original) A system according to claim 28, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising the public data of the or each further trusted party; each second computing entity being arranged, when satisfied that the policy defined by the encryption key string has been met so far as the associated trusted party is concerned, to provide a respective decryption key to the printer, the second computing entity concerned being arranged to generate this decryption key in dependence on the encryption key string and the private data of the associated trusted party; and decryption of the encrypted first data set by the printer requiring use of the decryption keys provided by all of the trusted parties.

33. (Original) A system according to claim 32, wherein said policy comprises a respective set of at least one condition associated with the or each trusted party, each second computing entity being arranged to be satisfied that said policy has been met when the set of at least one condition for the trusted party associated with the second computing entity concerned has been met.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

34. (Original) A system according to claim 32, wherein the first data set concerns a document to be published, the first computing entity and one of the second computing entities are both associated with a document publisher, and the printer is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the printer.

35. (Original) A system according to claim 28, wherein the first data set is encrypted using a bilinear pairing technique.

36. (Original) A system according to claim 28, wherein the first data set is encrypted using a quadratic residue technique.

37. (Original) A system according to claim 28, wherein the printer and the second computing entity are incorporated into the same item of equipment.

38. (Original) A system according to claim 28, further comprising a portable device comprising the second computing entity and a first communications interface, the printer comprising a second communications interface arranged to cooperate with the first communications interface to enable communication between the second computing entity and the printer; the communications interfaces being such that the portable device must be present at the printer for the communication between the second computing entity to take place.

Claims 39 and 40 (Cancelled)

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

IX. EVIDENCE APPENDIX

There is no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or any other evidence entered by the Examiner that Appellant is relying upon in this appeal.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

X. RELATED PROCEEDINGS APPENDIX

No decisions rendered by a court or the Board of Patent Appeals and Interferences are being submitted.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543